[19] 中华人民共和国国家知识产权局

[51] Int. Cl.
G06F 13/00 (2006.01)
G06F 15/16 (2006.01)

[12] 发明专利说明书

专利号 ZL 03123496.8

[45] 授权公告日 2008 年 2 月 6 日

[11] 授权公告号 CN 100367249C

[22] 申请日 2003.5.9 [21] 申请号 03123496.8

[30] 优先权

[32] 2002. 5.10 [33] US [31] 10/144，059

[73] 专利权人 微软公司

地址 美国华盛顿州

[72] 发明人 D·R·莫厄尔斯

D·杜布罗夫基尼 R·莱班

D·E·施密特 R·维斯瓦纳塔恩

J·E·布雷扎克 R·E·沃德

[56] 参考文献

CN1310410A 2001.8.29

US 5864665 A 1999.1.26

US5544322A 1996.8.6

US5864665A 1999.1.26

US5550981A 1996.8.27

审查员 何 博

[74] 专利代理机构 上海专利商标事务所有限公司

代理人 陈 斌

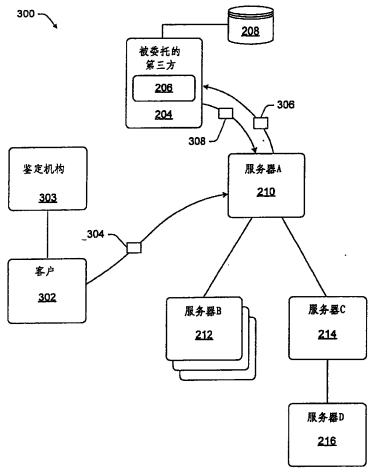
权利要求书 6 页 说明书 13 页 附图 6 页

[54] 发明名称

用于对计算机资源进行访问控制的方法和系统

[57] 摘要

提供了一些方法和系统，用于允许由被委托的外部服务加以身份认证的用户在受控层次上对所选择的本地计算资源进行访问，而不要求用户也具有关于各种资源的传统的访问控制性能。



1．一种用于提供对至少一个计算资源的访问控制的方法，其特征在于，包括：

接收与用户有关的一个唯一的标识符，所述用户将被提供访问所述至少一个计算资源而不要求所述用户具有与所述至少一个计算资源有关的一个唯一的本地用户帐户，所述唯一的标识符与已验证了所述用户身份的另一个计算资源有关；

将所述唯一的标识符翻译成一个安全标识符 SID；以及

确定所述 SID 是否与由与所述至少一个计算资源有关的访问控制机制提供的至少另一个 SID 相匹配。

2．如权利要求 1 所述的方法，其特征在于，所述唯一的标识符包括一个按照成对方式出现的唯一标识符 PUID。

3．如权利要求 2 所述的方法，其特征在于，所述 PUID 与一项“护照”服务有关。

4．如权利要求 3 所述的方法，其特征在于，将所述唯一的标识符翻译成所述 SID 还包括：

将所述 PUID 分成至少一个子权限标识符部分和至少一个成员标识符部分。

5．如权利要求 3 所述的方法，其特征在于，将所述唯一的标识符翻译成所述 SID 还包括：

将所述 PUID 提供给一个应用编程接口 API；以及

作为答复，从所述 API 接收所述 SID。

6．如权利要求 1 所述的方法，其特征在于，接收所述唯一的标识符还包括：

接收一个基于 Kerberos 的消息内的所述唯一的标识符。

7．如权利要求 6 所述的方法，其特征在于，在所述基于 Kerberos 的消息内的一个 PAC 中提供所述唯一的标识符。

8．如权利要求 6 所述的方法，其特征在于，所述基于 Kerberos 的消息与 S4U2 自我过程有关。

9．如权利要求 6 所述的方法，其特征在于，所述基于 Kerberos 的消息与 S4U2 代理过程有关。

10． 如权利要求 1 所述的方法，其特征在于，确定所述 SID 是否与由所述访问控制机制提供的所述至少另一个 SID 相匹配还包括：

将所述 SID 与一个访问控制清单 ACL 内的所述至少另一个 SID 进行比较，该访问控制清单与所述至少一个计算资源有关。

11． 如权利要求 1 所述的方法，其特征在于，接收与用户有关的所述唯一的标识符还包括：

为将要被提供访问所述至少一个计算资源的所述用户提供一个默认帐户。

12． 一种用于建立有关至少一个计算资源的访问控制许可的方法，其特征在于，包括：

接收至少一位用户的至少一个电子邮件地址，该用户将被同意至少有限地访问所述至少一个计算资源；

将所述电子邮件地址提供给至少一项被委托服务，该被委托服务能够根据所述电子邮件地址来输出与所述用户有关的一个唯一的标识符；

接收由所述被委托服务输出的所述唯一的标识符；以及

根据所述唯一的标识符来设置与所述至少一个计算资源有关的至少一个用户访问控制许可。

13． 如权利要求 12 所述的方法，其特征在于，设置所述至少一个用户访问控制许可还包括：

将所述唯一的标识符翻译成一个安全标识符 SID；以及

将所述 SID 与所述至少一个计算资源的至少一个访问控制清单 ACL 关联。

14． 如权利要求 12 所述的方法，其特征在于，所述唯一的标识符包括一个按照成对方式出现的唯一标识符 PUID。

15． 如权利要求 14 所述的方法，其特征在于，所述 PUID 与一项“护照”服务有关。

16． 如权利要求 13 所述的方法，其特征在于，所述唯一的标识符包括一个 PUID，将所述唯一的标识符翻译成所述 SID 还包括：

将所述 PUID 分成至少一个子权限标识符部分和至少一个成员标识符部分。

17. 如权利要求 14 所述的方法，其特征在于，所述唯一的标识符包括一个 PUID，将所述唯一的标识符翻译成所述 SID 还包括：

将所述 PUID 提供给一个应用编程接口 API；以及

随后从所述 API 收回所述 SID。

18. 如权利要求 12 所述的方法，其特征在于，接收所述唯一的标识符还包括：

接收一个基于 Kerberos 的消息内的所述唯一的标识符。

19. 如权利要求 18 所述的方法，其特征在于，所述基于 Kerberos 的消息内的一个 PAC 中提供所述唯一的标识符。

20. 一种用于将一个按照成对方式出现的唯一标识符 PUID 翻译成一个对应的安全标识符 SID 的方法，其特征在于，该方法包括：

在用户不具有本地帐户的第一服务器处从所述用户具有帐户的物理上不同的护照服务器接收所述 PUID，或通过默认用户帐户从所述用户接收所述 PUID，所述 PUID 是由所述护照服务器基于所述第一服务器提供给所述护照服务器的与所述用户有关的标识符创建的；

在所述第一服务器处将所述 PUID 再分为至少一个子权限标识符部分和至少一个成员标识符部分；以及

在所述第一服务器处将所述至少一个子权限标识符部分和所述至少一个成员标识符部分安排为所述 SID。

21. 如权利要求 20 所述的方法，其特征在于，将所述至少一个子权限标识符部分和所述至少一个成员标识符部分安排为所述 SID 还包括：安排所述 SID 具有所述子权限标识符、一个 HIWORD(MemberIDHigh)、一个 LOWORD(MemberIDHigh)和一个 MemberIDLow。

22. 如权利要求 20 所述的方法，其特征在于：还包括输出所述 SID。

23. 一种用于控制对至少一个计算资源的访问的系统，其特征在于，该系统包括：

存储器；以及

被有效地耦合到所述存储器的逻辑模块，所述逻辑模块包括：

接收与用户有关的一个唯一的标识符的装置，所述用户将要被提供对所

述至少一个计算资源进行受控访问而不要求所述用户具有与所述至少一个计算资源有关的一个唯一的本地用户帐户，所述唯一的标识符与已验证了所述用户身份的另一个计算资源有关；

用于将所述唯一的标识符翻译成一个安全标识符 SID 的装置；

用于确定如果所述 SID 与被存储在所述存储器中并与所述至少一个计算资源有关的至少另一个 SID 相匹配，则允许所述用户访问所述至少一个计算资源的装置。

24. 如权利要求 23 所述的系统，其特征在于，所述唯一的标识符包括一个按照成对方式出现的唯一标识符 PUID。

25. 如权利要求 24 所述的系统，其特征在于，所述 PUID 与一项“护照”服务有关。

26. 如权利要求 25 所述的系统，其特征在于，所述逻辑模块进一步包括将所述“护照”唯一标识符分成至少一个子权限标识符部分和至少一个成员标识符部分的装置。

27. 如权利要求 23 所述的系统，其特征在于，所述唯一的标识符是在一个基于 Kerberos 的消息内被接收的。

28. 如权利要求 27 所述的系统，其特征在于，所述基于 Kerberos 的消息内的一个 PAC 中提供所述唯一的标识符。

29. 如权利要求 27 所述的系统，其特征在于，所述基于 Kerberos 的消息与 S4U2 自我过程有关。

30. 如权利要求 28 所述的系统，其特征在于，所述基于 Kerberos 的消息与 S4U2 代理过程有关。

31. 如权利要求 23 所述的系统，其特征在于，被存储在所述存储器中的所述至少另一个 SID 是与所述至少一个计算资源有关的访问控制清单 ACL 的一部分。

32. 如权利要求 23 所述的系统，其特征在于，所述逻辑模块进一步包括将匿名帐户性能提供给将要被提供对所述至少一个计算资源的访问控制的用

户的装置。

33. 一种用于为至少一个计算资源设置访问控制许可的系统，其特征在于，该系统包括：

一个通信网络；

被有效地耦合到所述网络的第一个设备，所述第一个设备包括：

接受至少一位用户的至少一个电子邮件地址的装置，该用户将被同意至少对所述至少一个计算资源进行有限的访问而不要求所述用户具有与所述至少一个计算资源有关的一个唯一的本地用户帐户；

将所述电子邮件地址提供给所述网络，随后在所述网络上接收与所述电子邮件地址有关的一个对应的唯一的标识符的装置；

根据所接收的唯一的标识符来为所述用户设置与所述至少一个计算资源有关的至少一个访问控制许可的装置。

34. 如权利要求 33 所述的系统，其特征在于，还包括：

被有效地耦合到所述网络的至少另一个设备，所述另一个设备包括：提供能够从所述网络接收所述至少一个电子邮件地址的至少一项可信的服务的装置；将所述电子邮件地址转换为所述唯一的标识符的装置；以及将所述唯一的标识符输出到所述网络的装置。

35. 如权利要求 34 所述的系统，其特征在于，所述第一个设备进一步包括：将所述唯一的标识符翻译成一个安全标识符 SID，并将所述 SID 与所述至少一个计算资源的至少一个访问控制清单 ACL 关联的装置。

36. 如权利要求 35 所述的系统，其特征在于，所述唯一的标识符包括一个按照成对方式出现的唯一标识符 PUID。

37. 如权利要求 36 所述的系统，其特征在于，所述 PUID 是一个“护照”唯一标识符。

38. 如权利要求 37 所述的系统，其特征在于，所述第一个设备进一步包括：在翻译成一个对应的 SID 的期间内，将所述“护照”唯一标识符分成至少一个子权限标识符部分和至少一个成员标识符部分的装置。

39. 如权利要求 33 所述的系统，其特征在于，所述唯一的标识符是在一个基于 Kerberos 的消息内被接收的。

40. 如权利要求 39 所述的系统，其特征在于，在所述基于 Kerberos 的消息内的一个 PAC 中提供所述唯一的标识符。

用于对计算机资源进行访问控制的方法和系统

相关的专利申请

本专利申请涉及2001年6月20日提交的标题为《用于控制身份认证证书的授权范围的方法和系统》的第09/886,146号美国专利申请，该专利申请被包括于此，用作参考。

技术领域

本发明通常涉及计算机访问控制，尤其涉及用于根据用户的外部身份认证来为该用户提供一个本地系统授权上下文的方法和系统。

背景技术

访问控制对于计算机安全而言极为重要。为了保护计算机系统的完整性和重要数据的机密性，已执行各种访问控制方案，来防止未经授权的用户和怀有恶意的攻击者对计算机资源进行访问。

为确保计算机安全的全面性，经常在各种层次上执行访问控制。例如，在一台计算机的层次上，通常要求用户经历登录程序，在登录程序中，计算机确定该用户是否被授权使用这台计算机。此外，在计算机网络的层次上，通常要求用户经历用户身份认证程序，其目的是控制用户对各种网络服务的访问。即使在网络访问控制服务器已身份认证用户之后，用户也可能仍然必须请求关于特殊服务器的许可证，才能访问那项服务。已提议并执行基于不同协议（例如，Kerberos 5协议）的各种方案，用于通过用户身份认证来控制网络访问控制。

通常，计算机的用户登录和网络访问控制的用户身份认证是两个分开的程序。然而，为了将用户处理不同的访问控制方案的负担减到最小，有时一起执行用户登录和网络访问的用户身份认证。例如，如果在Kerberos协议下执行用户身份认证，那么，当用户登录到计算机时，计算机也可以启动Kerberos身份认证过程。在Kerberos身份认证过程中，计算机联系Kerberos密钥分配中心（KDC），来首先获得给用户的票许可票（TGT）。然后，计算机可以使用TGT从KDC那里获得自己的通话票。

随着网络的发展，已产生一种趋势：将多层服务器/服务计算机布置成处理客户计算机请求。一个简单的例子是：客户计算机经由互联网向“万维网”网站提出请求。这里，可能有处理该请求的格式化和有关商业规则的一个前端网

络服务器，以及为该网站管理一个数据库的一个后端服务器。关于附加的安全性，可以对网站进行配置，以便身份认证协议将证书（例如，用户的 TGT）和/或（可能）其他信息从前端服务器发送（或授权）给后端服务器。在许多网站和/或其他多层网络中，这种操作正变得日益普遍。

当所有的服务器/服务和客户都同意使用相同的身份认证程序时，授权和其他类似的技术很有用。但是，当今使用不止一个身份认证程序。第 09/866,146 号未授权的美国专利申请表现了用于控制授权的改进措施。

如果用户为网络/系统身份认证用户，那么，通常有一项或多项附加的授权访问控制检查，以防止用户访问他/她未经授权可以访问的资源。一旦用户已被身份认证并已通过可应用的访问控制，就称用户被“授权”。在某些系统中，例如，访问控制建立在具有各种服务和资源（即对象）的访问控制清单（ACLs）的基础上。ACL 通常包括访问控制项目（ACEs），其中可以包括零个或多个安全标识符（SIDs）。SIDs 可能与被允许访问对象的一位用户或几组用户有关。如果 ACL 中没有 SIDs，那么，将没有用户可以访问对象。如果 ACL 中有 SIDs，那么，至少能够产生一个匹配 SID 的用户将被允许访问对象。

这样，当被身份认证的用户登录时，（例如）通过生成与用户有关的一个标记（例如，访问标记），来为用户创建一个身份认证上下文。该标记通常包括与用户有关的 SIDs。例如，用户的标记可以包括被分配给用户的一个唯一的 SID，以及被分配给用户的营业部的一组 SID。当用户试图访问一个对象时，将该对象的 ACL 与用户的标记进行比较。如果用户的标记包括与对象的 ACL 内的一个 SID 相匹配的至少一个 SID，那么，用某种方式来授权被身份认证的用户访问对象。例如，用户可能已阅读和书写关于他/她的营业部的其他成员（即另一组成员）所建立的一个文件的许可。

这种授权方案往往很适用于被加以仔细控制和管理的系统。例如，公司内的企业层次计算机网络通常提供一种内聚性的环境，其中，用户和 ACLs 可以由集中式和/或分布式身份认证与访问控制系统加以仔细地控制。另一方面，关于大型网络（例如，互联网和/或另外值得注目的非内聚性网络），尤其当需要尽可能地为用户中的许多人服务（包括没有本地访问控制帐户的用户）时，身份认证和访问控制会困难得多。随着软件程序和资源向基于网络的服务发展，将会更加需要能够授权用户与这类网络服务有关的活动。

结果，需要被改进的授权方法和系统。较佳的是，这些方法和系统将允许由被委托的外部资源进行身份认证的用户在某种受控的层次上访问某些对象，而不要求用户也具备与对象有关的一个唯一的用户帐户。而且，这些方法和系统不应该使能够为大量用户提供对对象的访问的布置的可量测性发生严重的退化。

发明内容

这里提供各种被改进的方法和系统，它们允许由被委托的外部资源进行身份认证的用户在各个受控层次上访问所选择的对象，而不要求用户也具备一个唯一的本地用户帐户。这些方法和系统的实施不会使计算机系统和/或网络布置的可量测性发生严重的退化（这里计算机系统和/或网络布置被配置成为大量用户提供对各种资源的访问）。

例如，通过对至少一个计算资源提供访问控制的一种方法，可以满足上述的需求和其他需求。该方法包括：接收与正在寻求访问计算资源的用户有关的一个唯一的标识符。较佳的是，该唯一的标识符已由另一个计算资源建立，这另一个计算资源被认为是可信的并/或以某种方式为用户服务和经常身份认证用户。该方法包括：将所接收的唯一的标识符翻译成适用于保护计算资源的访问控制机制的一个安全标识符（SID）。该方法还包括：确定该 SID 是否与访问控制机制以前所存储的并与计算资源有关的至少另一个 SID 相匹配。在某些示范实施中，该唯一的标识符包括（例如）由微软公司所提供的“护照”服务使用的一个对方式的唯一标识符（PUID），访问控制机制使用访问控制清单（ACL）来建立被允许访问计算资源的用户或用户组。

根据本发明的某些其他实施，提供了一种方法，用于建立对至少一个计算资源的访问控制许可。这里，该方法包括：接收至少一位用户的至少一个电子邮件（e-mail）地址，该用户将被同意至少对计算资源进行有限的访问。该方法还包括：将该电子邮件地址提供给一项可信的服务，该服务能够根据该电子邮件地址来返回与这位用户有关的一个唯一的标识符。该方法包括：接收该唯一的标识符，然后根据该唯一的标识符来设置至少一个访问控制许可。这可以包括：（例如）将该唯一的标识符翻译成一个 SID，并使该 SID 与计算资源的至少一个访问控制清单 ACL 关联。

根据本发明的其他方面，提供了一种将 PUID 翻译成对应的 SID 的方法。该方法包括：接收 PUID，将它再分为至少一个子权限标识符部分和至少一个成员标识符部分，并安排该子权限标识符部分和成员标识符部分构成 SID。

还根据本发明的某些实施提供了一种用于控制对至少一个计算资源的访问的系统。该系统包括逻辑和存储器，可以将该逻辑和存储器配置成：接收与将被提供对计算资源的访问的用户有关的一个唯一的标识符，将该唯一的标识符翻译成一个安全标识符（SID），并确定该 SID 是否与被存储在存储器中并与计算资源有关的至少另一个 SID 相匹配。

提供某些示范系统，用于为计算资源设置访问控制许可。一种系统包括连接第一个设备和至少另一个设备的一个通信网络。将第一个设备配置成：接受

至少一位用户的一个电子邮件地址，该用户将被同意至少对计算资源进行有限的访问；在网络上将该电子邮件地址提供给另一个设备；在网络上从另一个设备接收与该电子邮件地址有关的一个对应的、唯一的标识符；并根据该唯一的标识符来设置与计算资源有关的至少一个访问控制许可。将另一个设备配置成：在网络上接收该电子邮件地址，将该电子邮件地址转换为唯一的标识符，并在网络上将该唯一的标识符输出到第一个设备。

附图说明

通过参考以下详细的描述并结合附图，可以更完整地了解本发明的各种方法和系统。在这些附图中：

图 1 是方框图，总体展示了适用于本发明的某些实施的一种示范计算机系统。

图 2 是方框图，描绘了在客户服务器环境内加以执行并适用于本发明的某些实施的一个用户服务代理（S4U2 代理）程序。

图 3A 是方框图，描绘了在客户服务器环境内加以执行并适用于本发明的某些应用的一个用户服务自我（S4U2 自我）程序。

图 3B 是方框图，描绘了在客户服务器环境内加以执行并适用于本发明的某些实施的一个用户服务自我（S4U2 自我）程序。

图 4 是示意图，描绘了适用于本发明的某些实施的一种示范消息格式的各个所选部分。

图 5 是示意方框图，描绘了根据本发明的某些示范实施的一种系统和程序，用于将本地访问控制提供给被委托的资源所身份认证的用户。

图 6 是示意方框图，描绘了根据本发明的某些方面的一种系统和程序（例如，如图 5 中所示）的一项示范运用，该系统和程序用于允许没有本地访问控制帐户的用户访问具有充分授权委托程度的某些资源。

具体实施方式

纵览

在身份认证用户/资源并/或为试图访问某些资源的用户提供一个授权上下文的过程中，可以执行这里所描述的一些示范方法和系统。

下一个章节描述了一种示范计算环境。那以后的章节简要描述了示范的 S4U2 代理技术和 S4U2 自我技术，它们是第 09/886,146 号关联未决的美国专利申请的主题。

其后，在附图中描述并示出根据本发明的某些方面的一些技术，用于提供一种新颖的授权方案。例如，提供了一些被改进的方法和系统，以允许由被委

托的外部服务进行身份认证的客户服务（例如，用户）在受控的层次上对所选择的本地服务器资源进行访问，而不要求客户服务也具有本地访问控制性能。将会明白，可以按各种方法来使用这里所描述的各种授权方案，以改进计算资源的安全性并提高用户访问由这些计算资源提供的服务的能力。

示范计算环境

参考附图，其中，类似的参考数字指示类似的元件，本发明被展示为在一个合适的计算环境中加以执行。虽然未作要求，但是，将在正由个人计算机执行的计算机可执行指令（例如，程序模块）的一般上下文中描述本发明。程序模块通常包括执行特殊任务或实施特殊的抽象数据类型的例行程序、程序、对象、部件、数据结构等。而且，精通该技术领域的人将会理解，可以用其他的计算机系统配置（包括手持设备、多处理器系统、基于微处理器的或可编程的消费电子设备、网络 PCs、小型计算机、大型计算机和类似物）来实践本发明。本发明也可以在分布式计算环境中得到实践，在该环境中，由通过通信网络而被连接的各个远程处理设备来执行任务。在分布式计算环境中，程序模块可以被定位在本地内存存储设备和远程内存存储设备中。

图 1 展示了合适的计算环境 120 的一个例子，可以对其实施随后所描述的方法和系统。

示范计算环境 120 只是合适的计算环境的一个例子，并非意在对这里所描述的被改进的方法和系统的使用或功能性的范围进行任何限制。也不应该将计算环境 120 解释成具有涉及计算环境 120 中所展示的任何一个部件或部件组合的任何从属性或要求。

这里被改进的方法和系统可用于许多其他通用或专用的计算系统环境或配置。可能合适的众所周知的计算系统、环境和/或配置的例子包括（但不局限于）个人计算机、服务器计算机、薄弱客户、密集客户、手持或便携式设备、多处理器系统、基于微处理器的系统、置顶盒、可编程的消费电子设备、网络 PCs、小型计算机、大型计算机、包括以上任何系统或设备的分布式计算环境，等等。

如图 1 所示，计算环境 120 包括采取计算机 130 的形式的一个通用计算设备。计算机 130 的部件可以包括一个或多个处理器或处理部件 132、一个系统存储器 134，以及将包括系统存储器 134 的各种系统部件耦合到处理器 132 的一个总线 136。

总线 136 表示几种类型的总线结构中的任何一种或多种总线结构，包括一个存储总线或存储控制器、一个外围总线、一个加速图形端口，以及使用各种总线构造中的任何总线构造的一个处理器或本地总线。举例来讲（不作限制），这类构造包括“工业标准结构”（ISA）总线、“微通道结构”（MCA）总线、“增强的 ISA”（EISA）总线、“视频电子标准协会”（VESA）本地总线，

以及也被称作“中层楼（Mezzanine）总线”的“外围部件互连”（PCI）总线。

计算机 130 通常包括各种计算机可读介质。这种介质可以是可由计算机 130 进行存取的任何可用的介质，它包括易失和非易失介质、可移动和不可移动介质。

在图 1 中，系统存储器 134 包括采取易失存储器（例如，随机存取存储器（RAM）140）和/或非易失存储器（例如，只读存储器（ROM）138）的形式的计算机可读介质。一个基本输入/输出系统（BIOS）142 被存储在 ROM 138 中，基本输入/输出系统 142 所包含的基本例行程序有助于在计算机 130 内的各个元件之间传递信息（例如，在启动期间）。RAM 140 通常包含可以立即被存取并/或目前正由处理器 132 进行操作的数据和/或程序模块。

计算机 130 还可以包括其他可移动/不可移动的易失/非易失计算机存储介质。例如，图 1 展示了用于从不可移动的非易失磁性介质（未示出，通常被称作“硬驱动器”）进行读取并对其进行书写的一个硬盘驱动器 144、用于从可移动的非易失磁盘 148（例如，“软盘”）进行读取并对其进行书写的一个磁盘驱动器 146，以及用于从可移动的非易失光盘 152（例如，CD-ROM/R/RW、DVD-ROM/R/RW/+R/RAM 或其他光学介质）进行读取或对其进行书写的一个光盘驱动器 150。硬盘驱动器 144、磁盘驱动器 146 和光盘驱动器 150 都通过一个或多个接口 154 而被连接到总线 136。

这些驱动器和有关的计算机可读介质为计算机 130 提供计算机可读指令、数据结构、程序模块和其他数据的非易失存储。虽然这里所描述的示范环境使用硬盘、可移动磁盘 148 和可移动光盘 152，但是，精通该技术领域的人应该理解，能够存储可由计算机进行存取的数据的其他类型的计算机可读介质（例如，盒式磁带、快闪记忆卡、数字录象磁盘、随机存取存储器（RAMs）、只读存储器（ROM）和类似物）也可以被用于示范操作环境中。

许多程序模块可以被存储在硬盘、磁盘 148、光盘 152、ROM 138 或 RAM 140 上，这些程序模块包括（例如）操作系统 158、一个或多个应用程序 160、其他程序模块 162 和程序数据 164。

可以在操作系统 158、一个或多个应用程序 160、其他程序模块 162 和/或程序数据 164 内执行这里所描述的被改进的方法和系统。

用户可以通过输入设备（例如，键盘 166）和定点设备 168（例如，“鼠标”）来将命令和信息提供到计算机 130 中。其他输入设备（未示出）可以包括话筒、操纵杆、游戏垫、圆盘式卫星电视天线、串行端口、扫描仪、摄像机等。这些和其他的输入设备通过与总线 136 耦合的用户输入接口 170 而被连接到处理部件 132，但也可以由其他接口和总线结构（例如，并行端口、游戏端口或通用串行总线（USB））来加以连接。

监视器 172 或其他类型的显示设备也经由一个接口（例如，视频适配器 174）

被连接到总线 136。除监视器 172 以外，个人计算机通常包括可以通过输出外围接口 175 而被连接的其他外围输出设备（未示出）（例如，扬声器和打印机）。

计算机 130 可以在使用与一台或多台远程计算机（例如，远程计算机 182）的逻辑连接的联网环境中进行操作。远程计算机 182 可以包括与计算机 130 有关的这里所描述的许多或所有元件和特点。

图 1 中所示的逻辑连接是局域网（LAN）177 和一般的广域网（WAN）179。这类联网环境在办公室、企业范围的计算机网络、内联网和互联网中很普遍。

当被用于 LAN 联网环境中时，计算机 130 经由网络接口或适配器 186 而被连接到 LAN 177。当被用于 WAN 联网环境中时，该计算机通常包括用于在 WAN 179 上建立通信的一个调制解调器 178 或其他装置。调制解调器 178（可能是内置的，也可能是外置的）可以经由用户输入接口 170 或其他合适的机制而被连接到系统总线 136。

图 1 中描绘了经由互联网的 WAN 的一项特殊的实施。这里，计算机 130 使用调制解调器 178，以便经由互联网 180 来建立与至少一台远程计算机 182 的通信。

在联网环境中，与计算机 130 或其各个部分有关的所描绘的程序模块可以被存储在一个远程内存存储设备中。这样，例如，如图 1 中所描绘的，远程应用程序 189 可以驻留在远程计算机 182 的一个存储设备上。将会理解，所表现和描述的网络连接起示范的作用，可以使用在各台计算机之间建立一个通信链接的其他装置。

示范的 S4U2 代理技术和 S4U2 自我授权技术的概述

现在，该描述将简要地把焦点放在用于控制客户服务器网络环境中的身份认证证书的授权范围的某些技术。在这个例子中，描述一种基于 Kerberos 的系统。这些 S4U2 代理技术和 S4U2 自我技术以及随后描述的授权技术可以或可以不在相同的系统中加以执行，并且，也可以在其他基于证书的身份认证系统中加以执行。

如上所述，如果具有客户的票许可票（TGT）和有关的文电鉴别码，则允许持票者代表客户向被委托的第三方（例如，密钥分配中心（KDC））请求票。这种未被限制的授权当前在具有被发送票授权方案的某些 Kerberos 实施中得到支持。

第 09/886,146 号美国专利申请记住这一点，描述了限制或更好地控制授权程序的一些方法和系统。授权程序可以通过用户服务代理（S4U2 代理）技术来加以控制，该技术允许服务器或服务（例如，前端服务器/服务）代表客户请求用于其他服务器/服务的服务票。S4U2 代理协议以一种可控制的方式有利地提供了被限制的授权，该方式不要求客户将 TGT 发送到前端服务器。另一项技

术是允许服务器向自己请求服务票的用户服务自我（S4U2 自我）协议，但在所产生的服务票中提供了客户的身份。例如，这样，已由其他身份认证协议进行身份认证的客户可以接收可被用于 S4U2 代理协议以便提供被限制的授权的服务票。对于 S4U2 自我技术而言，有两种示范形式—— 即“无证据”形式和“证据”形式。在无证据形式中，例如，通过使用对服务器保密的另一种安全/身份认证机制，委托服务器来身份认证客户。在证据形式中，KDC（或被委托的第三方）根据为服务器提供的、身份认证客户时所获得的有关客户的信息（证据）来执行身份认证。

所以，不管客户是否已由 Kerberos 或某个其他的身份认证协议进行身份认证，该客户都可以在 Kerberos 环境内访问服务器/服务。结果，可以在基本上只有 Kerberos 的环境中操作后端和/或其他服务器/服务。

现在参考图 2 中的方框图，它描绘了客户服务器环境 200 内的一个 S4U2 代理协议/程序。如图所示，客户 202 被有效地耦合到具有身份认证服务 206（例如，KDC、证书许可权限、域控制器和/或类似物）的一个被委托的第三方 204。身份认证服务 206 被配置成访问数据库 208 中所保存的信息。客户 202 和被委托的第三方 204 被进一步有效地耦合到一个服务器（即服务器 A 210）。注意，如这里所使用的，可混杂使用条款服务器和服务，来表示相同或类似的功能性。

在这个例子中，服务器 A 210 是多个其他的服务器的前端服务器。这样，如所描绘的，服务器 A 210 被有效地耦合到服务器 B 212 和服务器 C 214。如所展示的，服务器 B 212 可能是一项被复制的服务。此外，服务器 C 214 被进一步有效地耦合到服务器 D 216。

响应于用户在客户 202 处的登录，身份认证请求（AS_REQ）消息 220 被发送到身份认证服务 206，这与身份认证答复（AS_REP）消息 222 响应。在 AS_REP 消息 222 内是一个与用户/客户有关的 TGT。遵循相同或类似的程序（未示出），以身份认证服务器 A 210。

当客户 202 想要访问服务器 A 210 时，客户 202 将一个票许可服务请求（TGS_REQ）消息 224 发送到身份认证服务 206，身份认证服务 206 返回一个票许可服务答复（TGS_REP）消息 226。TGS_REP 消息 226 包括跟客户 202 和服务器 A 210 有关的一张服务票。随后，在应用协议请求（AP_REQ）消息 228 中，为了启动通信通话，客户 202 将服务票发送到服务器 A 210。这类过程/程序众所周知，因此，这里不作更加详细的揭示。

在某些系统中，为了支持授权，客户将需要为服务器 A 210 提供客户的 TGT，以允许服务器 A 210 代表客户 202 请求额外的服务票。对于 S4U2 代理协议而言，这并不是必要的。反而，当服务器 A 210 需要代表客户 202 访问另一个服务器（例如，服务器 C 214）时，服务器 A 210 和身份认证服务 206 根据 S4U2 代理协议来进行操作。

服务器 A 210 将 TGS_REQ 消息 230 发送到身份认证服务 206。TGS_REQ 消息 230 包括服务器 A 210 的 TGT 和从客户 202 那里接收的服务票，并识别客户 202 正在寻求访问的所需或目标服务器/服务（例如，服务器 C 214）。例如，在 Kerberos 中，有一个被定义的可扩展数据领域，它通常被称作“额外票”领域。这个额外票领域可以被用于 S4U2 代理协议中，以传送从客户 202 那里接收的服务票；KDC 选项领域可以包括一个标志或其他指示符，该标志或其他指示符指示接收 KDC 顺道访问将被用于提供客户身份的票的额外票领域。精通该技术领域的人将会认识到，这些或其他的领域和/或数据结构可以被用来将必要的信息传送到身份认证服务 206。

在处理 TGS_REQ 230 中，身份认证服务 206（例如）根据客户 202 所建立的一个“可发送标志”的值来确定客户 202 是否已批准授权。这样，通过在客户的服务票中存在可发送标志，可以实施每个客户的授权。如果客户 202 不想参与授权，那么，不将票标记为“可发送”。身份认证服务 206 将会尊重这个标志，作为一项客户发动的限制。身份认证服务 206 可以访问数据库 208 中的额外信息，该数据库定义了允许服务器 A 210 授权（或不授权）给客户 202 的所选择的服务。

如果身份认证服务 206 确定允许服务器 A 210 授权给目标服务器/服务，那么，将 TGS_REP 消息 232 发送到服务器 A 210。TGS_REP 消息 232 包括关于目标服务器/服务的一张服务票。这张服务票看起来好象是客户 202（例如）使用该客户的 TGT 直接从身份认证服务 206 请求得到的。但是，事实并非如此。反而，在满意被身份认证的客户实质上根据曾身份认证从客户 202 那里接收的并被包括在 TGS_REQ 消息 230 中的服务器 A 210 的服务票而参与该请求之后，身份认证服务 206 对数据库 208 中的类似/必要的客户信息进行访问。但是，由于客户信息被携带在客户的票中，因此，服务器只需要从该票复制数据。

在某些实施中，TGS_REP 消息 232 识别目标服务器/服务和客户 202，并且还包括采取特权属性证书（PAC）、安全标识符、Unix ID、“护照”ID、证书等形式的特殊化实施身份/用户/客户帐户数据等。例如，PAC 可以由身份认证服务 206 建立，或者只是从 TGS_REQ 消息 230 中曾经所包括的客户的服务票复制而成。将在以下所示的示范授权上下文建立方案中进一步描述“护照”ID 的使用。

PAC 或其他用户/客户帐户数据也可以被配置成包括与授权范围有关的信息。这样，例如，图 4 是说明性图表，描绘了具有一个标题 402 和一个 PAC 404 的 Kerberos 消息 400 的各个所选择的部分。这里，PAC 404 包括授权信息 406。如图所示，授权信息 406 包括复合身份信息 408 和访问限制信息 410。

例如，复合身份信息 408 可以包括有关授权程序的记录信息（例如，有关一个事实的指示，该事实是：服务器 A 210 曾代表用户/客户 202 请求服务票）。

这里，可以提供多个这样的记录信息，可以使用这些记录信息将有关多个授权程序的历史连串起来或对该历史进行识别。对于审查目的和/或访问控制目的而言，这类信息可能会很有用。

例如，如果客户 202 已直接或间接地通过服务器 A 210 来寻求访问服务器/服务，则可以结合访问控制机制来使用访问限制信息 410，以便有选择地允许对某些服务器/服务进行访问；如果正通过服务器 B 212 来间接地寻求服务器/服务，则不能这样做。这个特点增加了对身份认证证书的授权的额外的控制。

在以上例子中，客户 202 曾由身份认证服务 206 进行身份认证。但是，可以认识到，可能不会对其他客户进行这样的身份认证。图 3A 中描绘了这种情况的一个例子。这里，已使用一种不同的身份认证协议机制 303 对客户 302 进行身份认证。例如，身份认证协议机制 303 可以包括“护照”、加密套接字协议层（SSL）、NTLM、“摘要”或其他类似的身份认证协议/程序。这里，在这个例子中，假设：客户 302 选择访问一项目标服务，该目标服务碰巧是由服务器 C 214 提供的。使用以上所描述的 S4U2 代理协议可以满足这项选择，但仅仅在服务器 A 210 已完成/遵循一个 S4U2 自我协议/程序之后才如此。

具有 S4U2 自我协议的一个基本前提是：服务器（例如，服务器 A 210）能够为正在访问服务器并且服务器已身份认证的任何用户/客户而自我请求服务票。这里所描述的示范 S4U2 自我协议被配置成支持具有身份认证“证据”的客户和没有这种身份认证证据的客户。

在缺少可以由身份认证服务 206 进行评估的身份认证证据的情况下，服务器 A 210 将会需要“委托”客户 302。这样，例如，如果客户 302 具有服务器 A 210 能够使其生效的身份认证证书或类似的机制 304，那么，可以确定：客户 302 被“委托”。因此，服务器 A 210 实质上是身份认证客户 302。

接下来，服务器 A 210 将一个 TGS_REQ 消息 306 发送到身份认证服务 206，身份认证服务 206 为客户 302 自我请求服务票。作为响应，身份认证服务 206 建立包括所请求的服务票的一个 TGS_REP 消息 308。然后，在随后的 S4U2 代理协议/程序中使用所接收的服务票，以便为客户 302 向服务器 C 214 请求服务票。例如，在某些 Kerberos 实施中，这要求在 TGS_REP 消息 308 中设置一个可发送标志，以便允许发送该服务票。被委托的第三方也可以为客户 302 建立一个 PAC，然后可以将其包括在所产生的服务票中。

如果不存在有关客户 302’的身份认证证据，那么，服务器 A 210 可以在 TGS_REQ 消息 312 中包括这种证据，作为额外的预先身份认证数据。图 3B 中的环境 300’中用说明性方法描绘了这一点。这里，客户 302’将证据信息 310 提供给服务器 A 210。例如，证据信息 310 可以包括一个挑战/响应对话或由另一个“被委托”的实体建立的其他信息。一接收到证据信息 310 和随后的确认，身份认证服务 206 就将会同意向服务器 A 210 自己请求服务票。注意，在某些

实施中，通过使用证据，服务器可能可以为客户获得一个受限制的 TGT。

在某些 Kerberos 实施中，TGS_REP 消息 314 中的可发送标志将被设置为允许发送服务票。如果 TGS_REQ 消息 312 中曾提供一个 PAC，那么，它可以被用在服务票中；否则，身份认证服务 206（这里是一个 KDC）可能会根据证据信息 310 来建立一个 PAC。例如，在 S4U2 自我中，客户的身份被包括在预先身份认证数据中。可以为那个客户在 PAC 的构建中使用这个身份，并将其加入（为该客户）被发给服务器的服务票。

示范的授权上下文建立技术

现在，将把描述的焦点放在根据本发明的某些实施的示范方法和系统上。可以使用或不使用 S4U2 代理协议和/或 S4U2 自我协议来执行这些方法和系统。可以使用或不使用 Kerberos 来执行这些方法和系统。可以使用或不使用“护照”服务（由位于华盛顿的雷德蒙的微软公司提供）来执行这些方法和系统。精通该技术领域的人将会认识到，可以使用各种其他的协议和/或服务来执行这些技术。然而，在这些例子中，将假设：如果需要的话，可以利用这些协议和服务来支持授权上下文建立技术。

现在参考图 5，它是说明性方框图，描绘了与客户-服务器网络布置 500 有关的某些特点/功能/程序，客户-服务器网络布置 500 能够为用户提供一个授权上下文，否则，这些用户将无权访问某些资源。

如图所示，服务器 X 502 被有效地耦合到服务器 Y 504、与用户#1（U1）有关的第一位客户 506，以及与用户#2（U2）有关的第二位客户 508。在这个例子中，如虚线方框 510、512 和 514 所表示的，这些设备之间有几种委托关系。这样，例如，当 U1 登录到客户 506 和服务器 X 502 以便访问由服务器 X 502 提供的一个资源（例如，对象 516）时，客户 506 和服务器 X 502 被配置成建立委托关系 510。这个登录程序可以包括身份认证和访问控制。同样，当 U2 登录到客户 504 和服务器 Y502 时，客户 504 和服务器 Y 508 被配置成建立委托关系 512。此外，在这个例子中，服务器 X 502 和服务器 Y 504 能够经由被委托的第三方 204 而建立委托关系 514。但是，注意，这时，客户 508 与服务器 X 502 之间没有委托关系。

现在将使用图 5 和（稍后）图 6 来描述一个程序，以展示本发明的某些方面，这些方面允许客户 508 拥有具有服务器 X 502 的一个授权上下文，它允许 U2 访问对象 516。一个小圆圈内的连续的数字标识符旁边的箭头说明性地表示各个程序动作。在其他实施中，其中的一些动作可能会按不同的顺序发生。

如上所述，动作#0 是创建委托关系 510、512 和 514。可以按需要为某些操作有选择地创建这类委托关系。

在这个例子中，假设：U1 想要允许 U2 访问对象 516。U1 通过委托关系 510

而被授权访问对象 516，而这时，U2 没有被授权访问对象 516。而且，还需要避免将 U2 作为另一位被授权的用户加入服务器 X 502 的访问控制系统。例如，当 U1 想要允许 U2 访问 U1 的在线规划日程表（被主办，或通过 U1 的雇主而被提供）时，会发生这种情况。这里，雇主不想将一个新的、被授权的用户帐户加入其系统。

参考图 6，它是方框图 600，表现了与通过客户 506 而被提供给 U1 的一个图形用户接口（GUI）有关的某些典型的特点。在这个例子中，在登录到服务器 X 502 之后，为 U1 显示网页 602 或类似的屏幕。在网页 602 内，对象 516 呈现了显示有关 U1 的信息的一个日程表 GUI 604。U1 能够打开一张报名表 606，该报名表包括一个标识符输入领域 608 和（任选）一个或多个可选择的许可设置 610。在这里，U1 将启动最终将会允许 U2 访问对象 516 的程序。

U1 为 U2 输入一个标识符。在这个例子中，该标识符包括关于 U2 的唯一的“万维网”电子邮件地址（即，user2@hotmail.com）。这里所输入的标识符是关于微软公司所提供的 hotmail.com 服务的一位注册用户的。作为 hotmail.com 的一位注册用户，假定 U2 也具有一个与微软公司相对应的“护照”帐户。U1 也可以为 U2 就同意访问对象 516(在这里,例如一个在线规划日程表应用程序）方面定义一个或多个许可设置 610。当前，U1 已为 U2 设置了允许阅读的许可，现在返回到图 5，这个用户识别程序由客户 506 与服务器 X 502 之间的动作#1 表示。

服务器 X 502 发现 U1 已为 U2 提供一个 hotmail.com 标识符，并在动作#2 中与服务器 Y 504 进行通信，在这种情况下，它被假定为一种众所周知的“护照”服务器。这里，服务器 X 502 将标识符 user2@hotmail.com 提供给服务器 Y 504，并要求服务器 Y 504 提供一个对应的普遍唯一的“护照”用户身份（PUID）（也经常被称作“对方式的唯一 ID”）。在动作#3 中，服务器 Y 504 返回 U2 的 PUID（524）。如果委托关系 514 是一种基于 Kerberos 的关系，那么，可以在（例如）如前所述的一个 PAC 中返回 PUID。

现在，服务器 X 502 具有 U2 的 PUID。在动作#4 中，服务器 X 502 将该 PUID 翻译成适用于服务器 X 502 的本地身份认证系统的一个对应的 SID 522。如所展示的，对象 516 与 ACL 518 有关，具有包括 SID 522 的至少一个 ACE 520。

64 位 PUID 实际上包括一个 16 位“护照”域权限标识符和一个 48 位成员标识符。为了建立 SID，需要将域权限保存为一个分开的值。要实现这一点，可以将 MemberIDHigh 分成两个部分并将这两个部分建立为分开的子权限，例如，如下所示：

S-1-10-21-(HIWORD (MemberIDHigh)) – (LOWORD (MemberIDHigh))–MemberIDLow-0

在这个例子中，“S-1-10-21”是由 ntseapi.h 定义的一个新的标识符权限。

在这项示范实施中，ntseapi.h 是被用于建立微软®视窗®操作系统的一个标题文件，该操作系统包含被用来构建 PUID-SID 的这个 SID 值的定义。注意，这个标题通常将不会直接暴露给开发者。但是，在 winnt.h 中的平台 SDK 中公开发表了 ntseapi.h 中的声明。

这样，利用 PUID 或从一个“被委托”的来源返回的其他类似的标识符而创建的一个示范 SID 实质上识别采用一种唯一的组合以及与本地授权系统相兼容的一种格式的众所周知的子权限和成员用户。

在动作#5 中，U2 登录（被进行身份认证）到服务器 Y 504，并在此过程中接收 PUID 524。在动作#6 中，U2 使用一个默认的（例如，未知的或匿名的）用户帐户来与服务器 X 502 连接，并提供在请求或其他类似消息中包括 PUID 524 的信息（例如，在 PAC 中）。在动作#7 中，服务器 X 504 发现这个默认用户（U2）已提供一个 PUID，并且，作为响应，建立了一个对应的 SID 532，SID 532 随后被放在与正在寻求访问对象 516 的默认用户（U2）有关的标记 530 中。在某些实施中，通过将 PUID 传送给被称作“LsaLogonUser”的一个应用编程接口（API），来建立 SID。这个 API 返回该 SID。

在动作#8 中，通过将默认用户的标记 530 中的一个或多个 SID 与 ACL 518 中的一个或多个 SID 进行比较，服务器 X 502 确定这位默认用户（U2）是否具有可以访问对象 516 的合适的访问许可。这里，来自标记 530 的 SID 532 将与 ACE 520 中的 SID 522 相匹配。结果，在动作#9 中，为 U2 创建身份认证上下文 526，它根据可应用的许可设置来允许 U2 访问对象 516。因此，例如，U2 可以观看（阅读）U1 的规划日程表，并可以确定 U1 和 U2 下周是否能够共享午餐。U2 没有登录到服务器 X 502；由于 U2 不象 U1 那样拥有帐户，因此，U2 的确无法登录到服务器 X 502。在这种情况下，U2 的身份认证实质上建立在委托关系 510、512 和 514 的基础上，U2 的初始身份认证使用客户 508 和服务器 Y 504。同意 U2 对服务器 X 502 的访问控制实质上基于 U1 的被委托授权（在动作#0 中，通过客户 506 和服务器 X 502）以及在动作#3 中的提供 PUID 524 的过程中与服务器 Y 504 的委托关系。

使用 PUID 的好处之一是：在“护照”的 PUIDs 的受控分配的基础上，所产生的 SID 将在全球保持唯一和坚持。

总结

虽然已在附图展示并在详细的前文中描述了本发明的各种方法和系统的一些较佳实施，但是，将会理解，本发明不局限于所揭示的示范实施例，而在不脱离如以下权利要求书所陈述和定义的本发明的精神的前提下，可以进行许多调整、修改和替换。

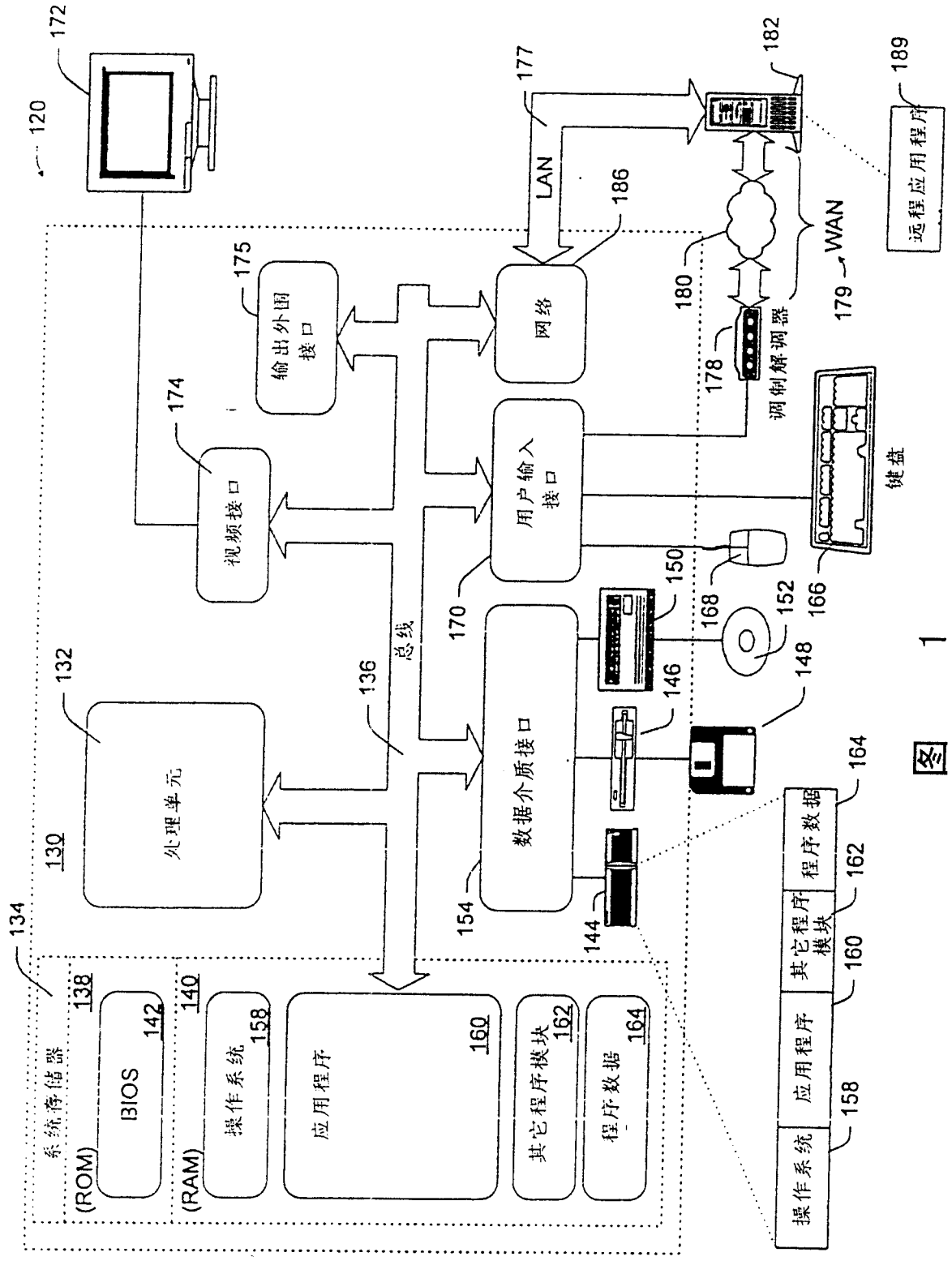

120
172
177
LAN
182
189
远程应用程序
186
网络
175
输出外围接口
180
WAN
179
174
视频接口
调制解调器
178
用户输入接口
键盘
150
168
152
166
总线
136
132
处理单元
170
数据介质接口
146
148
130
154
144
164
134
系统存储器
138
(ROM)
BIOS
142
140
(RAM)
操作系统
158
应用程序
160
其它程序模块
162
程序数据
164
操作系统
158
应用程序
160
其它程序模块
162
程序数据
164

图 1

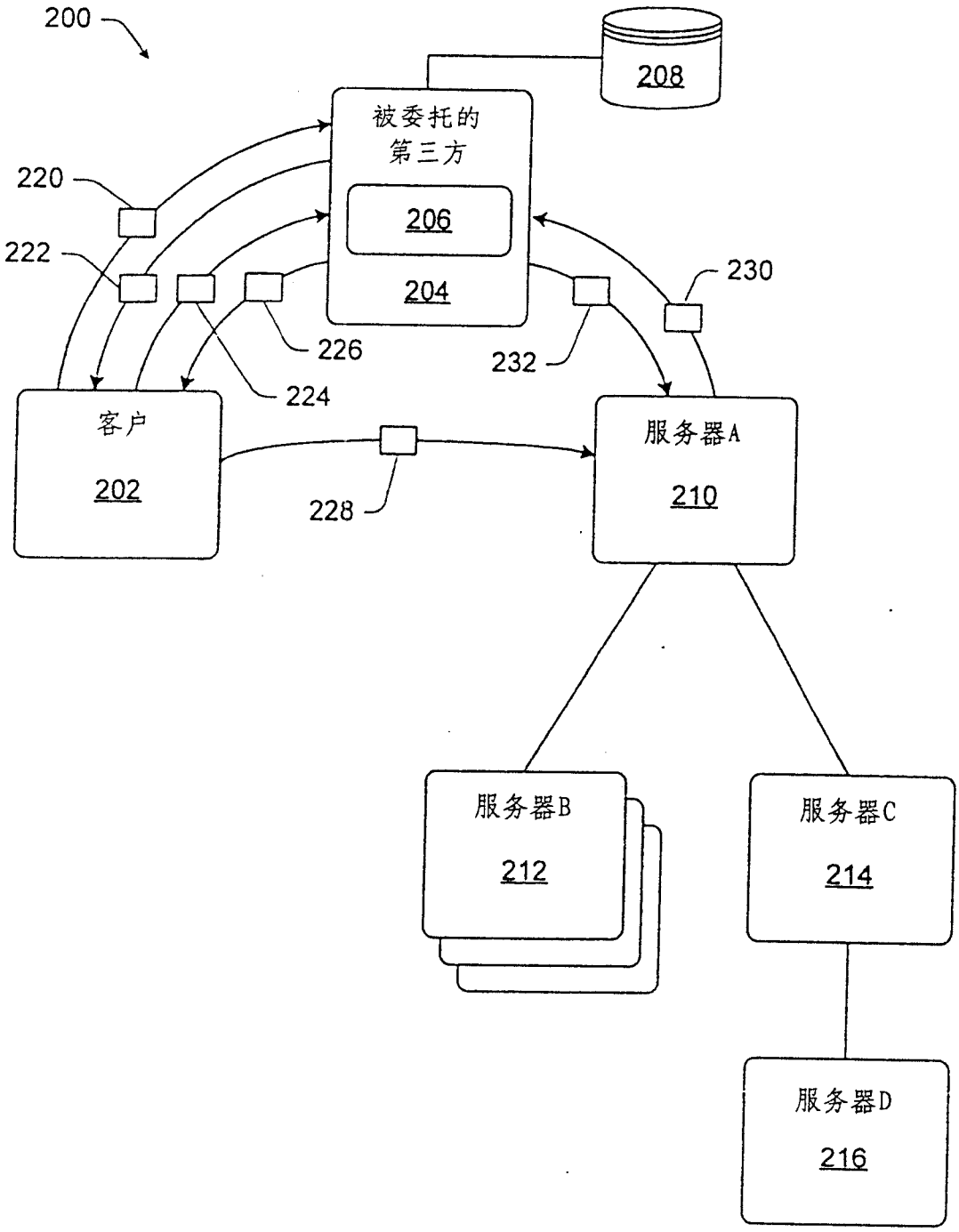

200
208
被委托的
第三方
206
204
220
222
230
226
232
224
客户
202
228
服务器A
210
服务器B
212
服务器C
214
服务器D
216

图 2

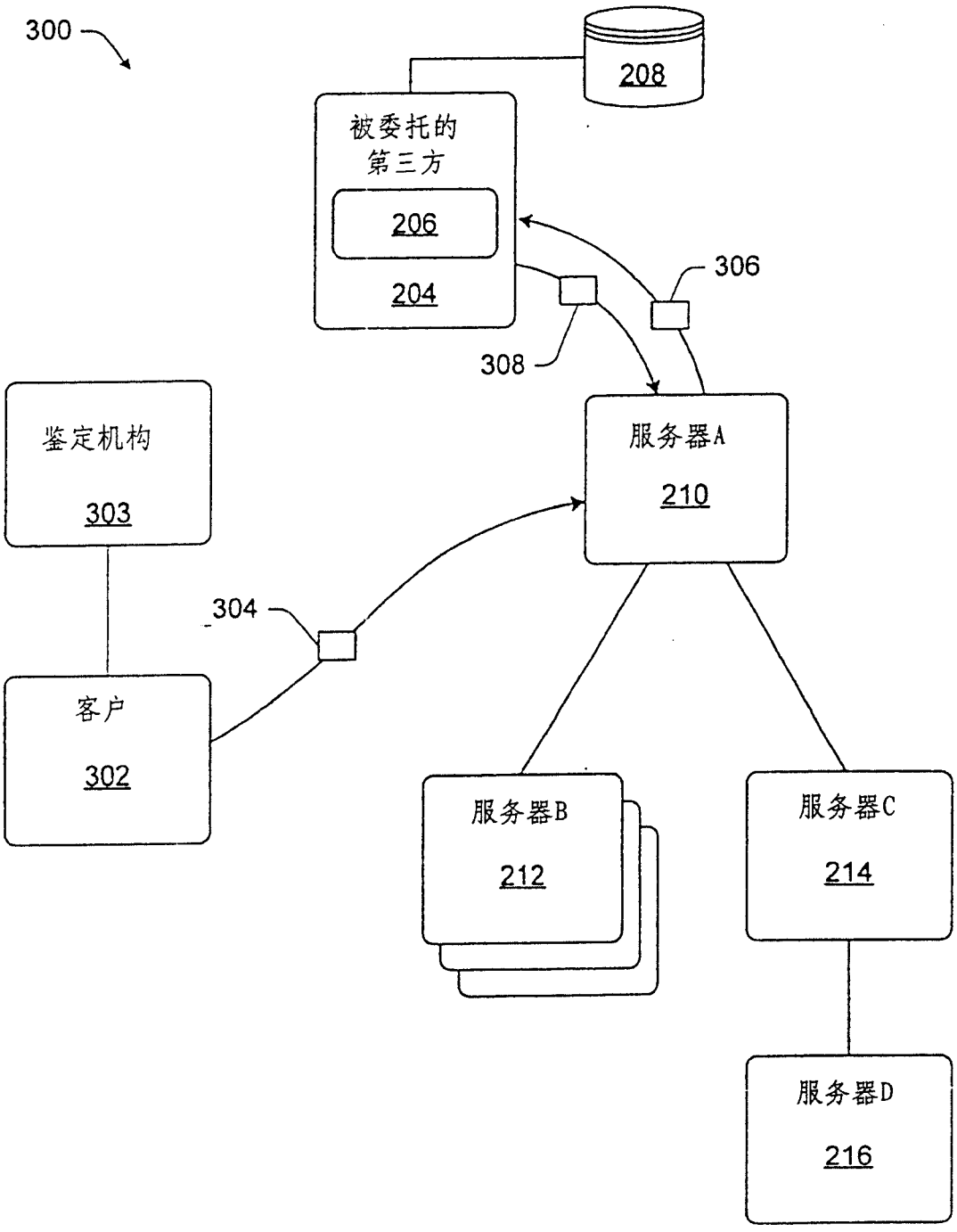

300
208
被委托的
第三方
206
204
306
308
鉴定机构
303
服务器A
210
304
客户
302
服务器B
212
服务器C
214
服务器D
216

图 3A

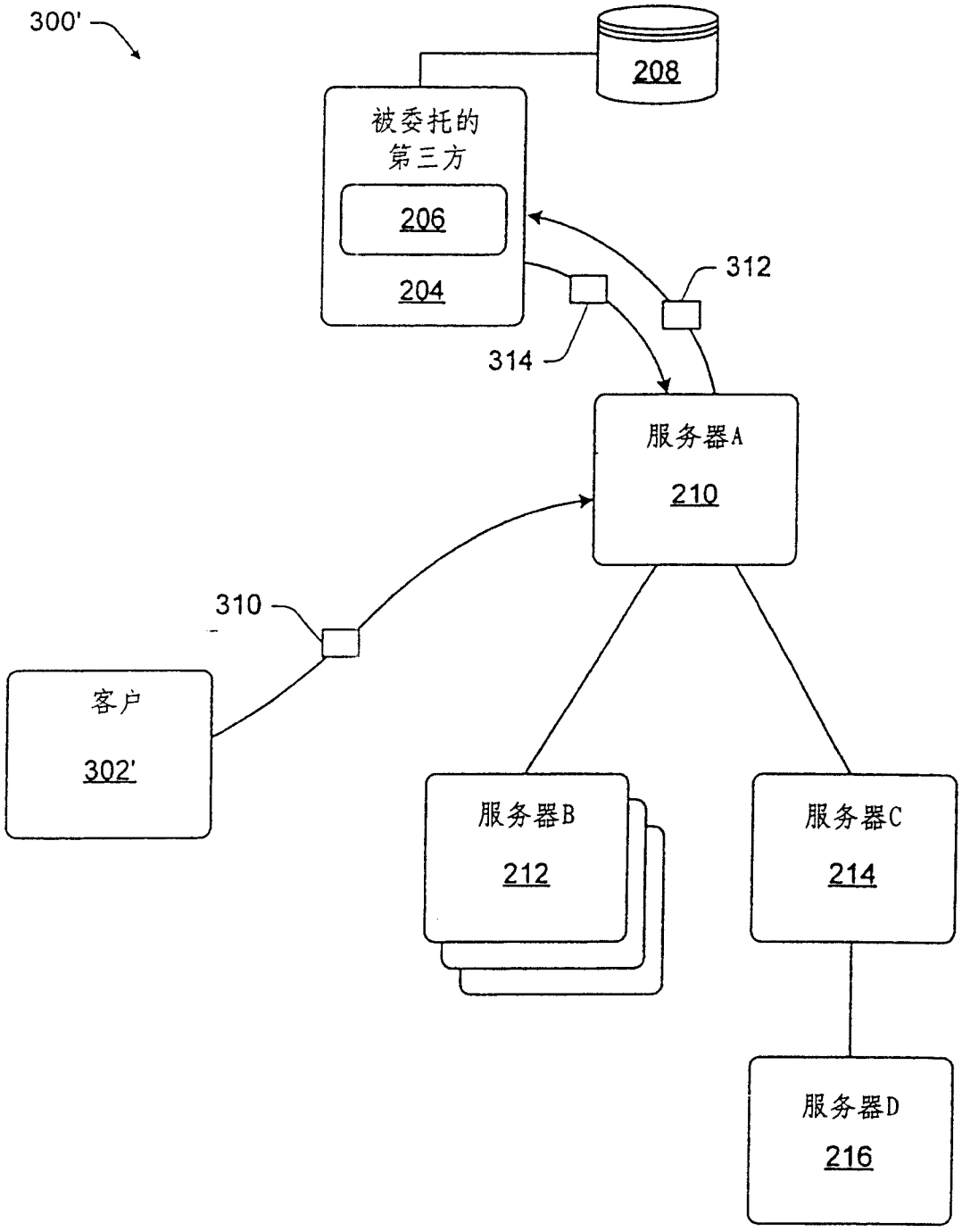

300'
208
被委托的
第三方
206
204
312
314
服务器A
210
310
客户
302'
服务器B
212
服务器C
214
服务器D
216

图 3B

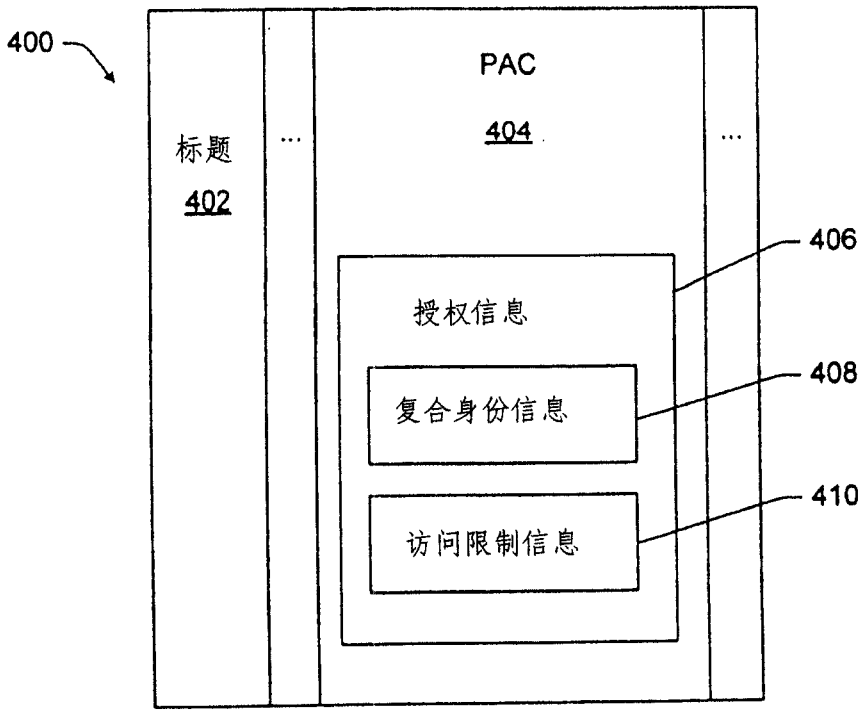

400
标题
402
...
PAC
404
...
406
授权信息
408
复合身份信息
410
访问限制信息

图 4

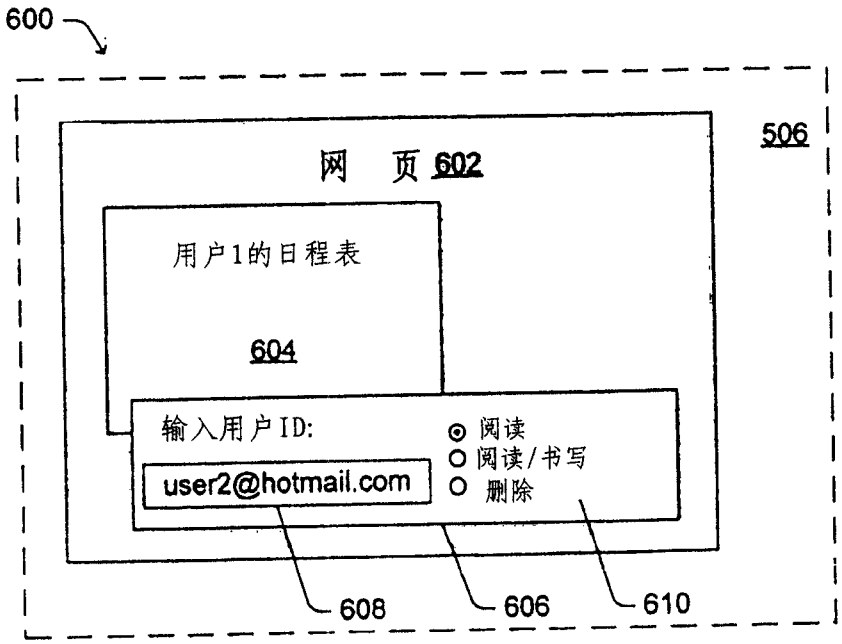

600
506
网 页 602
用户1的日程表
604
输入用户ID:
user2@hotmail.com
阅读
阅读/书写
删除
608
606
610

图 6

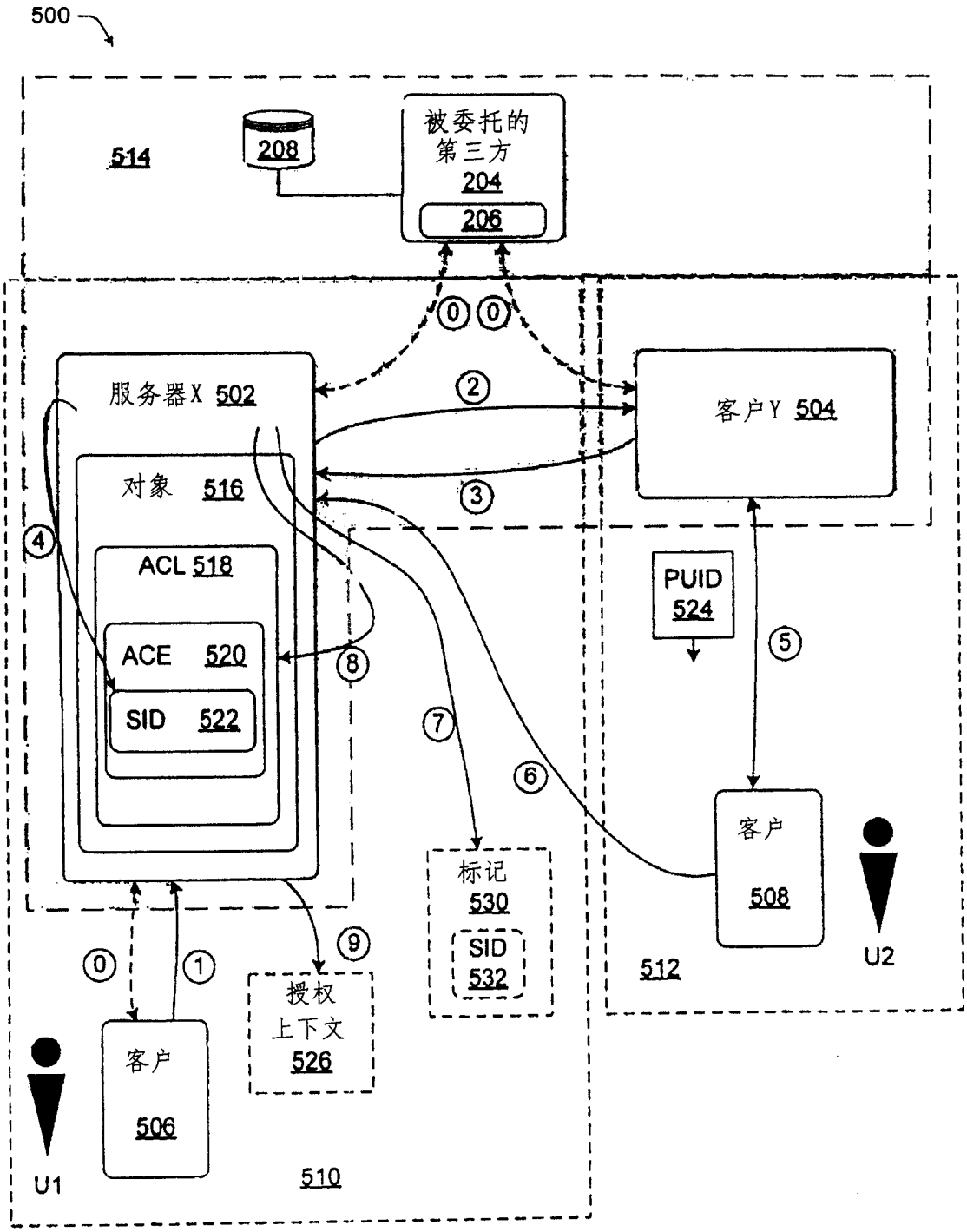

500
514
208
被委托的
第三方
204
206
0
0
服务器X 502
2
客户Y 504
对象 516
3
4
ACL 518
ACE 520
SID 522
8
PUID
524
5
7
6
客户
508
U2
512
标记
530
SID
532
0
1
9
授权
上下文
526
客户
506
U1
510

图 5